

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE POLICY DIRECTIVE 33-2

3 AUGUST 2011



Communications and Information

***INFORMATION ASSURANCE (IA)
PROGRAM***

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at <http://www.e-publishing.af.mil> for downloading and ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: SAF/A6O

Certified by: SAF/CIO A6
(Lt Gen William T. Lord)

Supersedes: AFPD33-2, 19 April 2007

Pages: 9

This Air Force Policy Directive (AFPD) implements Title III of Public Law 107-347, Federal Information Security Management Act (FISMA) of 2002, Department of Defense Directive (DoDD) 8500.01E, Information Assurance (IA), DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), DoDD 8521.01E, Department of Defense Biometrics, and DoDD 8570.01, Information Assurance (IA) Training, Certification, and Workforce Management. This directive applies to all military and civilian Air Force personnel; it also applies to the Air Force Reserve (AFR) and Air National Guard (ANG). This publication shall be applied to contractors or other persons through the contract or other legally binding agreement with the Department of the Air Force. Send all recommendations for changes or comments to SAF/A6O, 1800 Air Force Pentagon, Washington DC 20330-1800, through appropriate channels using AF Form 847, Recommendation for Change of Publication. Ensure all records created as a result of processes prescribed in this publication are maintained according to Air Force Manual (AFMAN) 33-363, Management of Records, and disposed of according to Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/rims.cfm>.

SUMMARY OF CHANGES

This document is substantially changed and must be reviewed in its entirety. The change is a policy directive update and establishes the Air Force IA program and risk management framework as an essential element to accomplishing the Air Force mission. The revision removed detailed IA information now published in AFI 33-200, Information Assurance (IA) Management and AFI 33-210, Air Force Certification and Accreditation (C&A) Program

(AFCAP). This directive addresses the Head of DoD Components responsibilities identified in DoD Directives in relation to Information Assurance.

1. Background. DoDD 8500.01E establishes the Defense IA Program pursuant to Title 10 United States Code Section 2224, which requires compliance with FISMA.

1.1. IA is defined as measures that protect and defend information and information systems (ISs) by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

1.2. Core IA disciplines consist of IA Awareness, Training, and Certification; Communications Security (COMSEC); Computer Security (COMPUSEC); Emission Security (EMSEC); and Risk Management Framework (including Certification and Accreditation (C&A)).

1.3. IA is associated with the Air Force Information Protection Program and its components of personnel, physical, industrial, and information security. IA, however, encompasses more than Information Protection. Air Force Doctrine Document (AFDD) 3-13, Information Operations, links IA to Information Operations as an integrated control enabler. Per AFDD 3-12, Cyberspace Operations, IA is also linked to Defensive Cyberspace Operations as a complementary function.

Note: The term “information assurance” as defined and used in the DoD and Air Force IA Programs is synonymous with the term “information security” as defined in the FISMA.

2. Objective. This directive establishes the Air Force IA program. IA is a risk management activity that must be balanced with operational need.

3. Scope. This directive applies to all information and ISs within Air Force purview, excluding non-Air Force space, Special Access Programs (SAP)/Special Access Requirements (SAR), and Intelligence community ISs. Space systems supporting only the Air Force are under the purview of the SAF/CIO A6. Non-Air Force space systems are multi-Component space systems (e.g., those supporting more than one DoD Component) and are under the purview of United States Strategic Command. Nothing in this directive shall alter or supersede the existing authorities and policies of the Director of National Intelligence regarding the protection of Sensitive Compartmented Information (SCI) and SAP for intelligence. The application of the provisions and procedures of this directive to SCI or other intelligence ISs is encouraged where they may complement or address areas not otherwise specifically addressed.

4. Policy. The Air Force IA program leverages fact-based operational risk assessments to ensure adequate safeguards and controls are implemented to ensure the availability, integrity, confidentiality, authentication, and non-repudiation of Air Force information and ISs in support of operational missions and business functions. Specific direction, details, procedures and guidance necessary to implement the Air Force IA program can be found in Air Force 33-2XX series instructions, applicable technical orders, and special security instructions. Total risk avoidance, based on Air Force IA strategy, is not practical and therefore risk assessment and management is required.

4.1. Consistent with its status in AFDD 3-13, as an integrated control enabler and in support of mission assurance as defined in AFDD 3-12, IA policy shall be aligned and synchronized

with NetOps, Information Operations, and Cyberspace Operations. IA policy will also be aligned and synchronized with Information Protection policy and guidance.

4.1.1. The Air Force will develop guidance to ensure the IA program and NetOps functions are executed consistent with the direction provided in DoDI 8410.02, NetOps for the Global Information Grid (GIG). The definition for NetOps outlined in DoDI 8410.02 will serve as the basis for delineating IA responsibilities under the guise of GIG Net Assurance versus “compliance and oversight” IA responsibilities (e.g., FISMA) supporting the federally-mandated functions of the Air Force Chief Information Officer.

4.1.2. Consistent with Air Force policy on Cyberspace Operations guidance (to be published under AFPD 10-17, Cyberspace Operations, and the Air Force 10-17XX series publications), the GIG Net Assurance functions outlined in this directive will complement the Defensive Cyberspace Operations component of Cyber Warfare.

4.2. Under the provisions of this directive the Air Force will:

4.2.1. Develop IA Implementation and Defensive Cyberspace Operations support guidance consistent with DoDI 8500.2, Information Assurance Implementation and DoDI O-8530.2, Support to Computer Network Defense. The guidance will be synchronized/deconflicted with Air Force Cyberspace Operations and Information Protection policy/guidance as appropriate.

4.2.2. Develop guidance for Space Systems and its portion of the Defense Acquisition System per DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, and DoDI 8581.01, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense. The Air Force will incorporate the guidance, as applicable, for instructions under this directive and Air Force policy on Information Protection (to be published under AFPD 16-14, Information Protection, and the Air Force 16-14XX-series publications).

4.2.3. Develop COMSEC and Cryptographic-related guidance, objectives, and standards consistent with DoDI 5200.16, Objectives and Minimum Standards for Communications Security (COMSEC) Measures Used in Nuclear Command and Control (NC2) Communications (U), DoDI 5205.08, Access to Classified Cryptographic Information, and DoDI 8523.01, Communications Security (COMSEC).

4.2.4. Develop EMSEC guidance, objectives, and standards consistent with DoDD C-5200.19, Control of Compromising Emanations and National guidance.

4.2.5. Incorporate the DoD Certification and Accreditation Program and IA Workforce Improvement Program into its guidance consistent with DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process, DoDD 8570.01, and DoD 8570.01-M, Information Assurance Workforce Improvement Program.

4.2.6. Develop guidance on Ports, Protocols, and Services Management, Biometrics, Public Key Infrastructure (PKI) and Public Enabling consistent with DoDI 8551.1, Ports, Protocols, and Services (PPSM), DoDD 8521.01E, and DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, respectively.

4.2.7. Develop guidance on Defense Industrial Base and security of unclassified DoD information on Non-DoD Systems consistent with DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA) Activities.

4.2.8. Develop guidance on the use of mobile code technologies consistent with DoDI 8552.01, Use of Mobile Code Technologies in DoD Information Systems.

4.2.9. Develop an IA governance structure and implement the Senior Risk Executive Function consistent with the DoD Risk Management Framework.

4.2.10. Ensure the concepts of reciprocity and reuse are implemented consistent with DoD IA policy and guidance.

5. Responsibilities.

5.1. Chief of Warfighting Integration and Chief Information Officer (SAF/CIO A6):

5.1.1. Develop, sustain, and maintain overall responsibility for the Air Force IA program consistent with DoDD 8500.01E and implements IA-related responsibilities designated for the Head of DoD Component as outlined in DoD 8000 series publications.

5.1.2. Develop guidance to ensure NetOps functions are executed consistent with the direction provided in DoDI 8410.02.

5.1.3. Develop, maintain, and enforce IA policies in accordance with statutory requirements outlined in the FISMA and serve as the Air Force focal point to DoD for all IA-related matters.

5.1.4. On behalf of SECAF, appoint Designated Accrediting Authorities (DAA), (e.g., Authorizing Officials) consistent with DoDD 8500.01E.

5.1.5. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise (DoDD 8500.01E).

5.1.6. Define IA performance measures to identify enterprise-wide IA trends (to include IA related vulnerabilities), plan of action and milestones (POA&M), and risk mitigation strategies (DoDI 8510.01).

5.1.7. Appoint the Senior Information Assurance Officer (SIAO) (e.g., Chief Information Security Officer) as mandated by DoDI 8510.01.

5.1.8. Submit the Air Force annual FISMA report to DoD CIO.

5.1.9. Approve Acquisition Information Assurance Strategies (DoDI 5000.02).

5.1.10. Ensure IA awareness training is provided to all Air Force personnel (DoDD 8500.01E).

5.1.11. Establish, resource, and implement IA training and certification programs for all Air Force personnel in accordance with DoDD 8570.01 and DoD 8570.01-M. These programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend, and retire DoD Information Systems.

5.1.12. Develop overarching guidance governing the operation of network assessments (red, blue, and green teams) and the IA Assessment and Assistance Program.

MICHAEL B. DONLEY
Secretary of the Air Force

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

Title 44 United States Code Sections 3541-3549 (Federal Information Security Management Act (FISMA))

Title 10 United States Code Section 2224, Defense Information Assurance Program
Public Law 107-347 (E-Government Act of 2002)

DoDD 4630.05, Interoperability and Supportability of Information Technology (IT) and National Security System (NSS), 5 May 2004

DoDD C-5200.19, Control of Compromising Emanations (U), 16 May 1995

DoDD 8000.01, Management of the Department of Defense Information Enterprise, 10 February 2009

DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 14 April 2004

DoDD 8500.01E, Information Assurance (IA), October 24 2002

DoDD 8521.01E, Department of Defense Biometrics, 21 February 2008

DoDD 8570.01, Information Assurance (IA) Training, Certification, and Workforce Management, 15 August 2004

DoD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005

DoDI 5000.02, Operation of the Defense Acquisition System, 8 December 2008

DoDI S-5200.16, Objectives and Minimum Standards for Communications Security (COMSEC) Measures Used in Nuclear Command and Control (NC2) Communications (U), 14 November 2007

DoDI 5205.08, Access to Classified Cryptographic Information, 8 November 2007

DoDI 5205.13, Defense Industrial Base (DIB) Cyber Security/Information Assurance (IA) Activities, 29 January 2010

DoDI 8410.02, NetOps for the Global Information Grid (GIG), 19 December 2008

DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2009

DoDI 8500.2, Information Assurance (IA) Implementation, 6 February 2003

DoDI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007

DoDI 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004

DoDI 8523.01, Communications Security (COMSEC), 22 April 2008

DoDI O-8530.2, Support to Computer Network Defense (CND), 9 March 2001

DoDI 8551.1, Ports, Protocols, and Services Management (PPSM), 13 August 2004

DoDI 8552.01, Use of Mobile Code Technologies in DoD Information Systems, 23 October 2006

DoDI 8580.1, Information Assurance (IA) in the Defense Acquisition System, 9 July 2004

DoDI 8581.1E, Information Assurance (IA) Policy for Space Systems Used by the Department of Defense, 21 June 2005

AFDD 3-12, Cyberspace Operations, 15 July 2010

AFDD 3-13, Information Operations, 11 January 2005

AFPD 16-14, Information Protection (Pending publication)

AFI 33-200, Information Assurance (IA) Management, 23 December 2008

AFI 33-210, Air Force Certification and Accreditation (C&A) Program, 23 December 2008

AFMAN 33-363, Management of Records, 1 March 2008

Air Force Records Information Management System Records Disposition Schedule (RDS)

Prescribed and/or Adopted Forms

AF Form 847, Recommendation for Change of Publication

Abbreviations and Acronyms

AFCAP—Air Force Certification and Accreditation Program

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFRIMS—Air Force Records Information Management System

AFSPC—Air Force Space Command

ANG—Air National Guard

C&A—Certification and Accreditation

CIO—Chief Information Officer

CND—Computer Network Defense

COMPUSEC—Computer Security

COMSEC—Communications Security

CS/IA—Cyber Security/Information Assurance

DAA—Designated Accrediting Authority

DIACAP—DoD Information Assurance Certification and Accreditation Process

DIB—Defense Industrial Base

DoD—Department of Defense

DoDD—Department of Defense Directive
DoDI—Department of Defense Instruction
EMSEC—Emission Security
FISMA—Federal Information Security Management Act
GIG—Global Information Grid
GNA—GIG Net Assurance
IA—Information Assurance
IS—Information System
IT—Information Technology
JP—Joint Publication
PK—Public Key
PKI—Public Key Infrastructure
POA&M—Plan of Action and Milestones
PPSM—Ports, Protocols, and Services Management
NC2—Nuclear Command and Control
NetOps—Network Operations
NSS—National Security Systems
OPR—Office of Primary Responsibility
RDS—Records Disposition Schedule
SAP—Special Access Programs
SAR—Special Access Requirements
SCI—Sensitive Compartmented Information
SECAF—Secretary of the Air Force
SIAO—Senior Information Assurance Official
WLAN—Wireless Local Area Network

Terms

Communications Security (COMSEC)—The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (JP 6-0)

Computer Security (COMPUSEC)—The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. (JP 6-0)

Cyberspace Operations—The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (JP 3-0)

Emission Security (EMSEC)—The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto equipment and telecommunications systems. (JP 6-0)

GIG Net Assurance (GNA)—The set of NetOps functions that includes the operational responsibilities for information assurance, computer network defense (to include computer network defense response actions), and critical infrastructure protection in defense of the GIG. . (DoDI 8410.02)

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services and National Security Systems. (JP 6-0)

Information Assurance (IA)—Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (JP 3-13, DoDD 8500.01).

Information Technology (IT)—Any equipment, or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a Component directly, or used by a contractor under a contract with the Component, which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term “IT” also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term “IT” does not include any equipment that is required by a Federal contractor incidental to a Federal contract. The term “IT” includes National Security Systems (NSS). (DoDD 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), May 5, 2004). Note: The above term is considered synonymous with the term “information system” as defined and used in Air Force programs.

Network Operations (NetOps)—Activities conducted to operate and defend the Global Information Grid. (JP 6-0). The DoD-wide operational, organizational, and technical capabilities for operating and defending the GIG. NetOps includes, but is not limited to, enterprise management, net assurance, and content management. NetOps provides commanders with GIG situational awareness to make informed command and control decisions. GIG situational awareness is gained through the operational and technical integration of enterprise management and defense actions and activities across all levels of command (strategic, operational, and tactical). (DoDI 8410.02)